CLAIMS

1. Method to provide an authentication for a user (U2) in a telecommunication network during session establishment according to a protocol between a user equipment (EQUIP) and an authentication device (AUTH), **characterized by**

- generating by said user equipment (EQUIP) a credential (C(P-U2; XID21) based upon a user password (P-U2) being associated to said user (U2) and a session parameter (XID21) being determined by said user equipment (EQUIP) for said session which is actual being established; and

- comprising in a session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) of said protocol (DHCP) a user identification (USER2) that uniquely identifies said user (U2), said session parameter (XID21) and said generated credential (C(P-U2; XID21)); and

-forwarding said session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) by said user equipment (EQUIP) to said authentication device (AUTH); and

- upon reception by said authentication device (AUTH) of said session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) verifying said received credential (C(P-U2; XID21)) with a generated verification credential (VC(P-U2; XID21)) based upon said received session parameter (XID21) and said user password (P-U2) being associated to said received user identification (USER2) and thereby providing said authentication for said user (U2).

2. The method to provide an authentication for a user (U2) according to claim 1, characterized in that said method further comprises also determining according to predefined rules and conditions an acceptance of said received session parameter (XID21).

3. The method to provide an authentication for a user (U2) according to claim 1, characterized in that said protocol (DHCP) is a Dynamic Host Configuration Protocol.

4. The method to provide an authentication for a user (U2) according to claim 1, characterized in that said session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) is a Discover message of a Dynamic Host Configuration Protocol.

5. The method to provide an authentication for a user (U2) according to claim 4, characterized in that said user identification (USER2), said session parameter (XID21) and said generated credential (C(P-U2; XID21)) being included as a predefined Option in an Option field of said Discover message.

6. The method to provide an authentication for a user (U2) according to any previous claim characterized in that said session parameter (XID21) is a session identifier that uniquely identifies said session that is actual being established.

7. A user equipment in a telecommunication network to enable an authentication for a user (U2) during session establishment according to a protocol (DHCP) between said user equipment (EQUIP) and an authentication device (AUTH), **characterized by** that said user equipment (EQUIP) comprises

- a first generator (GEN1) to generate a credential (C(P-U2; XID21) based upon a user password (P-U2) being associated to said user (U2) and a session parameter (XID21) being determined by said user equipment (EQUIP) for said session which is actual being established; and

- a second generator (GEN2) to comprise in a session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) of said protocol (DHCP) a user identification (USER2) uniquely identifying said user (U2), said session parameter (XID21) and said generated credential (C(P-U2; XID21)) and to forward said session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) to said authentication device (AUTH) in order to enable thereby said authentication device (AUTH), upon reception of said session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) to verify said received credential (C(P-U2; XID21)) with a generated verification credential (VC(P-U2; XID21)) based upon said received session parameter (XID21) and said user password (P-U2) that is associated to said received user identification (USER2) and to provide thereby said authentication for said user (U2).

8. An authentication device (AUTH) to provide an authentication for a user (U2) in a telecommunication network during session establishment according to a protocol (DHCP) between a user equipment (EQUIP) and said authentication device (AUTH), **characterized by** that said authentication device (AUTH) comprises

a third generator (GEN3) to generate a verification credential (VC(P-U2; XID21)) based upon a received session parameter (XID21) and based upon a user password (P-U2) that is associated to a received user identification (USER2), and to provide said verification credential (VC(P-U2; XID21)) to a verifier (VER); and

said verifier (VER) coupled to said third generator (GEN3) to verify said verification credential (VC(P-U2; XID21)) against a received credential (C(P-U2; XID21)) and to provide thereby said authentication for said user (U2);

said received user identification (USER2), said received session parameter (XID21) and said received credential (C(P-U2; XID21)) being

comprised by said user equipment (EQUIP) in a session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) of said protocol (DHCP),

said credential (C(P-U2; XID21) being generated by said user equipment (EQUIP) based upon said user password (P-U2) that is uniquely associated to said user (U2) and said session parameter (XID21) that is determined by said user equipment (EQUIP) for said session which is actual being established;

said session message (DISCOVER(USER2; XID21; C(P-U2; XID21))) being forwarded by said user equipment (EQUIP) to said authentication device (AUTH).

9. The authentication device (AUTH) according to claim 8, characterized in that said authentication device is at least partly included in a network access provider (NAP).

10. Telecommunication network to provide an authentication for a user (U2), **characterized** in that said telecommunication network comprises anyone of a user equipment (EQUIP) according to claim 6 and an authentication device (AUTH) according to claim 7 or claim 8.